UAV Functional Requirements Document for Autonomous Earth Science Missions

Table of Contents

1.0 Preface

The concept of a "Functional Requirements Document" is defined in various ways – depending on the particular institutions or groups involved with generating and using it. For the current document, the team used the "Access 5 Functional Requirements Document" (Rev 1, dated September 5, 2003) as a primary guide for determining the format and type of material to be included. As such, the current document attempts to summarize the requirements of the overall system and each major element of the system in a way that:

- Describes the functional capability required
- Does not reference the use of specific technology for meeting that capability
- Describes the benefit of (or reasons for) specifying a particular capability
- Does not provide engineering performance specifications

The intent is for the current document to describe what the system must do, without specifying how it will be done – and without setting particular performance specifications for software or hardware. The logical follow-on to this document would be a "System Requirements Document" which would define particular engineering specifications for the system appropriate to the anticipated state of development for the relevant technologies over the time frame of the program.

2.0 Introduction

2.1 Background

Within NASA, the Earth Science Enterprise has long sought to use Unmanned Aerial Vehicles (UAVs) for science and application missions to complement other measurement platforms, including manned aircraft and satellites. There are key science issues for which the required data cannot currently be obtained from existing platforms. These include high altitude atmospheric composition measurements, and earth surface events at inaccessible locations or over long periods of time.

The Concept of Operations (CONOPS) document for the UAV Autonomous Earth Science Missions provides descriptions for several typical missions, flight phase requirements, and mission metrics. Although the initial emphasis was on high altitude missions, it was recognized that there are significant benefits associated with the ability of UAVs to operate in conditions too dangerous for manned aircraft. Therefore the CONOPS document also includes consideration of low altitude science missions and disaster monitoring – such as might be associated with a forest fire.

The purpose of this Functional Requirements Document (FRD) is to take the mission definitions described in the CONOPS document, and convert them into initial functional requirements for science or application mission UAV systems that could operate routinely within the existing constraints of the National Airspace System (NAS).

2.2 System Overview

For the purpose of this document, a UAV system will be defined as having the following four elements:

- the Air Vehicle Element,
- the Payload Element,
- the Science Mission Interface (SMI), and
- the Operator Interface.

While the system's Control Architecture spans all of the above elements, it is not broken out into a separate element here; it is included collectively in the requirements of the four elements. In general, the Control Architecture must facilitate transforming the goals specified by the human operators into actions taken by the system, and this will be satisfied by meeting the element requirements.

NAS components such as radar and radio communications equipment are anticipated to be part of the operating environment, but are not treated as a distinct UAV system functional element herein. Likewise, mission-relevant resources such as satellites (communications, observation) and scientific databases are presumed to be significant to the detailed design of the system, but are not specified in this document.

2.2.1 Air Vehicle Element

The Air Vehicle Element includes the UAV platform, the necessary onboard avionics hardware and software to ensure safe and efficient operation within the NAS, and all onboard supporting subsystems needed to successfully complete the UAVs intended mission.

2.2.2 Payload Element

The Payload Element is part of the Air Vehicle Element – but is defined as that portion which includes the onboard sensors, processors, and support systems associated with obtaining the specific data defined by the particular UAV mission objective. In many cases the payload element is also distinguished by being a separate "package" which can be removed from the Air Vehicle Element and replaced with another Payload Element.

2.2.3 Science Mission Interface (SMI)

The SMI provides personnel participating in the UAV mission with an interface to the payload sensors, and to any external data sets, personnel, or sources of information necessary for the accomplishment of that mission. The SMI affords the means to observe and interpret data obtained by the onboard sensors and processors; to observe and interpret mission-related data from sources external to the UAV system; to direct the onboard sensor systems; to communicate with other team members; and to integrate data evaluations by team members into mission planning.

The SMI will typically include items on the Air Vehicle Element and ground-based equipment or software. In some cases it may also include systems located on other aircraft or satellites.

2.2.4 Operator Interface

For very simple UAV systems the Operator Interface may be the same as the SMI, and for complicated systems it is expected that the UAV operator would still make use of the SMI for obtaining critical mission-related information. However, in general the Operator Interface is distinguished from the SMI by the following:

- The Operator Interface is primarily associated with control of the overall UAV within the NAS, whereas the SMI is primarily associated with communication among mission team members, and data acquisition, assessment, or processing.
- Vehicle control associated with the Operator Interface will typically be restricted to a single person having pilot-in-command responsibility – although there may be provision for transferring that responsibility.
- For security and safety reasons, the Operator Interface may have security and redundancy requirements beyond what is needed for the SMI

2.3 Basic Assumptions

The UAV Sector Roadmap states that "100% Autonomy" is a key 15-year goal for the Vehicle Systems program. For the purpose of developing the requirements set forth in this document, the following interpretations and assumptions were made:

- "100% autonomy" is considered to mean that during all operations, (and at the discretion of the operator) the vehicle shall be able to operate autonomously – requiring operator intervention only as an exception, or at defined decision points or events. This includes responding to non-normal situations, including emergencies, although such responses may be limited by degraded system capabilities.

- The functional requirements developed are to reflect what is needed to provide performance, reliability, and security appropriate for a manned aircraft of equivalent class and category conducting comparable operations – or appropriate to the risk level presented by a system failure when there is no equivalent class of manned aircraft.

The rationale associated with these two assumptions is described in greater detail in the document sections defining the functional requirements for the individual elements of the UAV system.

3.0 Functional Requirements

3.1 Air Vehicle Element

The Air Vehicle Element includes the UAV platform, the necessary avionics hardware and software to ensure safe and efficient operation within the NAS, as well as anything needed to safely and successfully complete the UAVs intended mission. As a top level requirement, the air vehicle element shall not present or create a hazard to other aircraft in flight or persons and/or property on the ground, greater than that created by manned aircraft of equivalent class and category – or appropriate to the risk level presented by a system failure when there is no equivalent class of manned aircraft.

3.1.1 Conventional Aircraft Subsystem Requirements

Vehicle subsystems that perform functions essentially indistinguishable from analogous functions performed on a manned aircraft shall satisfy performance and reliability requirements appropriate to a manned aircraft of equivalent class and category conducting comparable operations. Examples of these subsystems include the airframe and structures subsystem, propulsion subsystem, flight control subsystem, position estimation subsystem, and path-steering subsystem (i.e. guidance and autopilot/auto throttle subsystems)

Rationale: As a new class of vehicle, it is advantageous if UAVs can minimize the need for special regulatory and policy accommodations by looking as much like current certified vehicle classes as practical. This implies that like manned aircraft, a Functional Hazard Assessment be done to identify Minor, Major, Severe and Catastrophic failure conditions that may arise as a result of a malfunction or failure to function. The consequence of a failure condition determines the minimum required integrity for the system responsible for this function. A failure condition classified as minor may not require any fault tolerance; a catastrophic failure condition (i.e. resulting in loss of vehicle control) will almost certainly require a fail-operational capability.

3.1.2 Payload Interface Requirements

The vehicle shall support payload interface requirements including power, environmental, and flight operations and constraints as defined in the Payload FRD

Rationale: Ensures harmonization of vehicle and payload FRDs . That said, the system engineering function should carefully manage this interface to ensure the requirements and implementation are considered across these segments. Certain requirements like sensor pointing and tracking precision might be optimized through requirements allocated to both segments.

3.1.3 UAV Specific Requirements

3.1.3.1 Operator Interface Support

The vehicle shall normally operate under the supervision of a remote "operator" having responsibilities equivalent to the "Pilot in Command" as defined in CFR14 Part 91.3 and who shall be the final authority as to the operation of the vehicle. The vehicle shall afford this operator sufficient situation awareness and control authority to fulfill her responsibility. The operator interface specifications needed to fulfill this requirement can be found in the Operator FRD.

Rationale: Simplifies harmonization of vehicle and operator FRDs. For the foreseeable future (15-20 years out), it is likely that the FAA and insurers will require a responsible (i.e. liable) operator to oversee UAV operations.

3.1.3.2 Routine Autonomous Operation

During routine operations and at the discretion of the operator, the vehicle shall be able to operate autonomously, requiring operator intervention only as an exception or at defined decision points or events. This capability requires the ability to autonomously resolve routine conflicts with static and dynamic obstacles such as other traffic, adverse weather, and terrain/obstructions while balancing mission considerations such as remaining within a given air mass or directing a sensor at a designated target. Routine autonomous operation shall include all phases of flight including take-off and landing at appropriately equipped facilities and ground operations including pre- and post-flight checks and surface movements. As implied in the operator's FRD and requirement 3.1.3.1 above, the vehicle automation shall be capable of notifying the operator when additional operator monitoring or intervention is required to maintain design safety margins. Such notification must occur with sufficient time for the operator to formulate an appropriate course of action. Also as defined in the operator's FRD, the vehicle must be designed to afford the operator an independent means of monitoring its status and health.

Rationale: The vehicle's automation should function as first officer or co-pilot with the operator as captain. The vehicle should be capable of performing routine tasks with sufficient awareness to recognize when reaching boundaries of its design capabilities and authority or when future actions require value judgments best left to the responsible human operator. The automation system must be able to effectively explain its reasoning to the operator. In addition, the vehicle must provide sufficient raw information to the operator to enable independent monitoring of its functioning

3.1.3.3 Non-Normal Operations

Systems for dynamic prediction, prevention, detection and mitigation shall allow in-flight system reconfiguration and response to failures in the UAV sub-systems and structures within critical time constraints. Such response should include dynamic reallocation of processing and sensing resources to maintain critical functions in the presence of both anticipated and unanticipated malfunctions and failures. The monitoring systems shall provide status information to the mission management system and to the operator.

In keeping with the design philosophy of not presenting or creating a hazard to other aircraft in flight or persons and/or property on the ground, greater than that created by manned aircraft of equivalent class and category, operational conditions (e.g.. hazardous weather such as icing, wind shear) and failure conditions not shown to be extremely improbable shall not compromise the ability to safely operate in, or extract the vehicle from, the air space environment. Depending on the nature of the failure(s) and the remaining capability of the vehicle, extraction may be achieved through a range of means such as precautionary landing, engagement of a flight recovery system, or activation of a flight-termination system once over an unpopulated area.

Rationale: This is a restatement of the basic design requirement not to present new hazard levels beyond those present with manned aircraft. Special emphasis is placed on the effects of hazardous operational conditions and significant failure conditions.

3.1.3.3.1 Non-normal Operations with link with Remote Operator

During non-normal operations with a functioning link to the Remote operator, the vehicle shall be designed to provide graceful performance degradation and minimize changes to the operator's ability to command the vehicle. At the same time, the vehicle shall be designed to minimize the probability of autonomously responding to, or providing the operator with, hazardously misleading information or control actions.

Rationale: The vehicle should do what it can to assist the operator in her role as PIC without creating additional hazards like reacting to an erroneous sensor.

3.1.3.3.2 Non-normal Operations without link to Remote Operator

In the event of lost communication between the vehicle and the remote operator, the vehicle shall autonomously take action to minimize any additional risk to other aircraft or persons and/or property on the ground and shall be designed to minimize any adverse operational impact on other airspace users and air traffic controllers. If communication cannot be reestablished within a specified interval, the vehicle shall activate the FRS in a predictable fashion to reduce risk and operational impact on the NAS and persons and property on the ground to nominal as soon as practicable.

Rationale: This is the really challenging situation with no existing certification precedents to follow. The vehicle's response will be highly dependent on the capabilities of its technology and ability to react autonomously without adult supervision.

3.1.3.3.3 Flight Recovery System

The vehicle shall incorporate a system capable of expeditiously removing the UAV from the NAS in the event that the vehicle becomes uncontrollable. The system shall provide levels of contingency operation such that catastrophic termination of flight is employed as a last resort. The FRS shall operate independently of the primary flight control computer, and in the event of flight control computer hardware or software failure, shall be capable of flying the aircraft to a pre-determined safe recovery zone, attempting a landing at a pre-determined site, and if required commanding the aircraft into such controlled termination maneuver as is possible given the failure state. The FRS shall progress deterministically through recovery tactics, unless commanded by the Remote Operator to execute a specific operation.

Rationale: The vehicle should attempt self-preservation as long as it safe to do so, with provision for catastrophic termination should it become necessary. Given that control of the UAV is completely dependent on a large amount of software, the FRS should be independent of the main systems.

3.1.3.4 Security of vehicle control

Control of the vehicle by unauthorized parities shall be considered a catastrophic failure condition and the corresponding probability of such a failure shall be no more than allowed for catastrophic failure conditions for manned aircraft of equivalent class and category. Security shall include the communication link with the remote operator and components affecting the vehicle's autonomous behavior.

Rationale: 9/11.

3.2 Payload Element

3.2.1 Air Vehicle Interface

The payload shall interface with UAV hard points, power distribution and communication networks configured to enable mission capability. Standardized electrical, mechanical and software payload interfaces are desirable.

Rationale: Payload integration is critical to mission success.

3.2.2 Operations

The payload shall nominally operate remotely and autonomously of human control. If the payload can be externally configured or controlled, it shall accept such input from the SMI.

Rationale: Independent operation is required since no operator is on board to monitor mission progress, payload system status and configuration, product generation and data quality. A very simple payload may not afford any external control. However, for more complex systems the capability for human control must be preserved so that users of the payload data can direct the payload when desired.

3.2.3 Monitoring

The payload system shall monitor, record and communicate in-situ and remotely sensed geophysical (and engineering) data.

Rationale: Science measurements as required by the mission. Raw data archiving is required by the science team.

3.2.4 Data Processing

The payload shall selectively develop, analyze and communicate onboard data to:

- Provide real time data products
- Provide flight re-planning guidance
- Ensure quality
- Monitor collection process
- Provide a closed feedback loop with the on-board avionics

Rationale: Real time feedback required to ensure mission success.

3.2.5 SMI Interface

The payload shall interface with SMI to:

- Develop and provide flight re-planning guidance
- Ensure quality
- Monitor collection progress
- Unambiguously prioritize conflicting SMI and avionics payload tasking directions using a rule-based, quasi AI system

Rationale: SMI provides virtual forum to interactively interface with payload, and aircraft to ensure mission success.

3.3 Science Mission Interface (SMI)

The SMI provides personnel participating in the UAV mission with an interface to the payload systems, and to any external data sets, personnel, or sources of information necessary for the accomplishment of that mission. The SMI affords the means to visualize, observe and interpret data obtained by the payload; to visualize, observe and interpret mission-related data from sources external to the UAV system; to direct the payload systems (and indirectly the UAV); to communicate with other team members; and to integrate sensing goals into mission planning.

3.3.1 Configuration Options

3.3.1.1 Integral With Operator Interface

The SMI interface may be integral with the Operator Interface.

Rationale: For a simple, locally controlled and monitored UAV, there may be a single interface to the vehicle and the sensor systems.

3.3.1.2 Distributed

Sensor data customers shall be able to interact with other elements of the UAV operations team (e.g. operator, mission director, other data customers) using the SMI.

Rationale: The SMI may not be co-located with the Operator Interface; there may be multiple, distributed, collaborative data customers. Keeping all members of the team cognizant of the vehicle and sensor status is required for mission success.

3.3.2 UAV Sensor Interface Requirements

3.3.2.1 Near-Real Time Communication

The SMI shall provide a real-time or near-real-time interface to the payload systems– although the level at which the data is available may be very dependent on the particular mission.

Rationale: This is the means for customers of the UAV's data products to interact with the data-producing hardware and software during the mission. On-board processing may allow samplings or summaries of data to be available through the SMI

3.3.2.2 Controllability

If the payload systems are controllable, the SMI shall provide the means to direct those systems.

Rationale: Inputs to the payload might be anything from very high-level commands to an autonomous sensor controller, to low-level commands to re-configure a particular piece of hardware, but the SMI should be able to handle all possible interactions. This could be as simple as a command line, or as sophisticated as a point-and-click graphical interface.

3.3.2.3 Status & Functionality Access

The state of the payload systems, including any autonomous functionality, shall be accessible through the SMI.

Rationale: Payload data consumers are likely to want to know what the payload systems are doing, think they are doing, or are planning to do, in addition to the actual data products.

3.3.2.4 Remote Reconfiguration

If the system has the capacity for remote reconfiguration, selection and configuration of payload data products shall be possible through the SMI.

Rationale: Not all payload products are necessarily required in all mission phases; requirements may change dynamically; failures may require intervention.

3.3.2.5 Data Access

All payload data products required for the specified mission shall be accessible through the SMI.

Rationale: The SMI should ideally provide a fused view of all data products, and there should only be one interface to all products. There may be products that do not need to be accessed for a given mission, but anything that is needed must be available through the SMI

3.3.2.6 Multi-Platform Interface

Design of the SMI shall allow for multi-UAV interaction when required for a particular mission.

Rationale: It is possible that the payloads of more than a single UAV could form a distributed sensor, or that the payloads of more than one UAV could be controlled from a single location, or that data from multiple UAVs, individually controlled, could be viewed in several locations.

3.3.3 Mission Team Communication Requirements

3.3.3.1 Data Customers

When mission planning includes sensing goals, the data customer shall be able to contribute to the mission planning via the SMI.

Rationale: The data customer may desire to specify the sensing goals, which then must be incorporated into the mission plan; the data customer should be able to do this from within the SMI and have those goals integrated into the overall plan.

3.3.3.2 Data Access and Visualization

When required for particular missions, the SMI shall provide access to particular internal and external data sets, systems, or personnel. The SMI will provide multi-source visualization abilities, and will utilize NASA and industry standard protocols to retrieve data from other space and land based sources.

Rationale: To support efficient, real-time decision making, additional data and/or information resources must be accessed, and their contents merged with the payload data stream, allowing for both tactical and strategic information spaces. Access to specific weather information, satellite data, expert consultation, etc. . may be required during the time frame when the mission is being conducted.

3.4 Operator Interface

This element does not currently address control of, or interaction with, multiple UAVs or swarms. The Operator's role and actions in initiating and terminating a mission are also not defined.

3.4.1 Situational Awareness

The operator interface shall provide the situational awareness required to monitor the progress of all ground and flight phases during the mission.

Rationale: An operator must have adequate situational awareness to safely and intelligently manipulate the air vehicle system on the ground and in the air to meet mission requirements. The operator should have the same level of situational awareness as a flight crew flying a manned aircraft.

3.4.1.1 Health Monitoring

The operator shall be able to monitor the health of all safety- and mission-critical sensors and systems, including the payload, air vehicle (power, avionics, structural) and mission management system.

Rationale: Critical requirement for knowing when an RTB should be issued, or when to terminate the vehicle. Fuel state, cg should be included as well as failure modes.

3.4.1.2 Onboard Decision Process Monitoring

The operator shall be able to monitor the decision making process of the autonomous systems, including current and predicted mode or system state.

Rationale: In order to monitor the behavior of the system, it is critical for the operator to know what mode the system is in, and the reasons for changing to a new mode.

3.4.1.3 Weather Information Access

The operator shall be able to communicate with real-time weather information and weather forecasting for the purpose of modifying the mission profile of the air vehicle.

Rationale: Real-time weather information is safety critical, and can also be crucial in some science missions for getting the required data.

3.4.1.4 ATC Communication

The operator shall be able to communicate with ATC, and comply with instructions from ATC during all ground and flight phases of the mission.

Rationale: ATC concerns may require real-time adjustments to your flight path. This includes all phases of flight, including the ability to command a holding pattern upon entering the terminal flight phase area while waiting for clearance to land.

3.4.1.5 Detection & Avoidance

The air vehicle shall be able to sense and respond to air traffic and obstacles that may intersect with the air vehicle's flight path for the purpose of collision avoidance. Contingency sensing capability shall be provided for the ground operator.

Rationale: In the terminal area, especially, the ability to sense other aircraft or other obstacles on take-off, approach, and taxi is critical to safety.

3.4.2 Safe Conduction of Ground & Flight Operations

The operator interface shall provide the capability to safely conduct ground and flight operations, and execute research missions.

3.4.2.1 Modification to Mission Profile

The operator shall be able to modify in real-time the mission profile of the vehicle in any ground or flight phase.

Rationale: As an example scenario, imagine you are flying along the pre-flight mission trajectory and the real-time science data or weather indicate that a point of interest is developing in another location. This requirement allows the operator to re-direct the air vehicle to that point of interest. An assumption here is that the mission profile includes any maneuvers, (i.e. spiral descent) which are required for collecting data.

3.4.2.2 Default Mission Profile

The operator shall be able to return control of the air vehicle to the pre-flight mission profile.

Rationale: As you investigate points of interest you may want the vehicle to return to the original plan. This requirement allows that to be easily implemented.

3.4.2.3 Contingency Plans

The operator shall be able to command the air vehicle to execute contingency plans during any ground or flight phase.

Rationale: If the science sensors or something else fails, or weather isn't as favorable as predicted for collecting data, the operator should be able to call it a day. Several levels of contingency with different priorities would be implemented such as, RTB, loiter in place, auto-return and auto-land, go-around, aborted take-off, etc.

3.4.2.4 Flight Recovery System

The operator shall be able to activate a Flight Recovery System capable of terminating flight without undue hazard to other aircraft, human life, and/or property on the ground.

Rationale: If the vehicle has a loss of control you need to be able to recover or terminate it before it crashes into a populated area. If you recover or terminate the vehicle, you want to do so with enough information to be able to minimize the damage, and prevent casualties. This also implies that information would be provided to the operator to determine where the vehicle will impact and the implications thereof.

3.4.2.5 Emergency Procedures

The operator interface shall allow the pilot/operator to assume command and to take appropriate action in the event of a system failure. This requirement is similar to that existing for manned aircraft.

Rationale: As a last resort, the vehicle would become a remotely operated aircraft. This option cannot be used in some failure scenarios (lost link for example). Also, during the developmental stage, this capability would allow envelope expansion, and an incremental build-up approach to full capability.

3.4.3 Communication With Mission Team Members

The operator shall be able to communicate with science team and/or payload data for the purpose of re-directing the mission profile of the air vehicle.

Rationale: Input from the science data, whether it be a communication from a scientist or a display of science data directing the operator, is necessary for getting the most 'bang for the buck'.

3.4.4 Communication Link Failure

3.4.4.1 Single-Fail Tolerant

The communication link between the operator and the air vehicle shall be single-fail tolerant.

Rationale: This link is critical for flight safety so it must be redundant, at least.

4.0 Acronyms & Abbreviations

AC	Aircraft
AGL	Above Ground Level
AIRDAS	Airborne Infared Disaster Assessment System
ARP	Autonomous Rotorcraft Project
ATC	Air Traffic Control
ATIS	Automatic Terminal Information Service
CFR	Code of Federal Regulations
SMI	Science Mission Interface
CONOPS	Concept of Operations
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FCC	Federal Communications Commission
FL	Flight Level
FRD	Functional Requirements Document
FRS	Flight Recovery System
FTS	Flight Termination System
GPS	Global Positioning System
HALE	High Altitude Long Endurance
IFR	Instrument Flight Rules
LASE	Low Altitude Short Endurance
MODIS	Moderate Resolution Imaging Spectroradiometer
NAS	National Airspace System
NASA	National Aeronautics & Space Administration
PIC	Pilot In Command
QA	Quality Assurance
RTB	Return to Base
SAR	Synthetic Aperture Radar
SMI	Science Mission Interface
TBD	To Be Determined
UAV	Unmanned Aerial Vehicle
VTOL	Vertical Take Off & Landing
Wx	Bad Weather